Math 776, Homework 4

(**) indicates it is open-ended and/or a hard problem.

1. (Local Kronecker-Weber Theorem- 2-adic case)
   This problem finishes the proof of local Kronecker-Weber theorem for the case of cyclic 2-extensions $[K : \mathbb{Q}_2] = 2^k$, for some $k \geq 1$.
   (a) For $m \geq 1$ show there is a unique unramified extension $K_u/\mathbb{Q}_2$ with Galois group $\mathbb{Z}/2^m\mathbb{Z}$. Show there is a totally ramified extension $K_r$ with Galois group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^m\mathbb{Z}$, namely $\mathbb{Q}_2(\zeta_{2^{m+2}})$.
   Conclude there is an abelian extension $K$ of $\mathbb{Q}_2$ having Galois group $(\mathbb{Z}/2\mathbb{Z})^3$.
   (b) Suppose there is a cyclic extension $K$ with Galois group $\mathbb{Z}/2^m\mathbb{Z}$ that is not contained in $K_r, K_u$ and derive a contradiction. Show first that the existence of such $K$ implies there exists an extension of $\mathbb{Q}_2$ with Galois group one of $(\mathbb{Z}/2\mathbb{Z})^4$ or $(\mathbb{Z}/4\mathbb{Z})^3$.
   (c) Use Kummer theory on these two types of Kummer extensions to rule out either of these Galois groups. The case $(\mathbb{Z}/2\mathbb{Z})^4$ corresponds to four independent quadratic extensions of $\mathbb{Q}_2$. Prove there are at most 3 independent quadratic extensions.
   (d) To rule out a field $N/\mathbb{Q}_2$ with Galois group $(\mathbb{Z}/4\mathbb{Z})^3$ we must adjoin a fourth root of unity $\sqrt{-1}$, and analyze Kummer extensions. Show that necessarily $\sqrt{-1} \in N$ in this case, which simplifies things. (You may also need to know or show that $A^2 + B^2 = -1$ has no solutions in $\mathbb{Q}_2$.)


2. (Infinite Galois Extensions-1 ) Let $L/k$ be a (possibly) infinite Galois extension with Galois group $G = \text{Gal}(L/k)$ with the Krull topology, i.e. open subgroups are $\text{Gal}(L/E)$ where $E$ is a finite Galois extension.
   (a) Prove basic open sets are open and closed. Deduce that $G$ is totally disconnected. Prove $G$ is compact.
   (b) Prove that each extension field $K/k$ inside $L$ has $K$ the fixed field of a closed subgroup $G'$ of $G$, and conversely.
   (c) Prove that each finite extension field $K/k$ with $K \subset L$ is the fixed field of an open subgroup of $G$, and conversely. [Thus all open subgroups are closed, and are of finite index in $G$.]
   (iv) Prove that $K/k$ is a normal extension if and only if $H = \text{Gal}(L/K)'$ is a normal closed subgroup of $G$.
   (v) Let $H$ be a finite index subgroup of $\text{Gal}(L/k)$. Must $H$ be an open subgroup?

3. (Infinite Galois Extensions-2 ) Let $L/\mathbb{Q}$ be the maximal abelian extension. Pick $\alpha \in G$, and suppose it is of infinite order. What can you say about:
(a) The closure $\bar{H}$ of $H = \langle \alpha^n : n \in \mathbb{Z} \rangle$ in $G$. Is there any simple relation between $H$ and $\bar{H}$?

(b) The normal extension $L^H$ corresponding to $\bar{H}$.

[How does the Galois group being abelian simplify things?]

4. (Infinite Galois Extensions-3)

For each prime $p$, let $\mathbb{Q}[p]$ be the maximal extension of $\mathbb{Q}$ that embeds into $\mathbb{Q}_p$. This is the compositum of all finite extensions $K/\mathbb{Q}$ with $K = \mathbb{Q}(\theta)$ generated by an algebraic integer $\theta$ whose minimal polynomial splits into linear factors (mod $p$).

(a) Show that $\mathbb{Q}[p]$ is an infinite extension of $\mathbb{Q}$ that is a Galois extension.

(b) (***) Say whatever you can about the structure of $Gal(\mathbb{Q}[p]/\mathbb{Q})$.

(c) (***) Say whatever you can about the structure of $Gal(\mathbb{Q}/\mathbb{Q}[p])$.

[Questions to ask: Say something about the structure of the Galois group as a profinite group. Or say something about how much of the maximal abelian extension of $\mathbb{Q}_p$ is inside $\mathbb{Q}[p]$, etc. Or to identify interesting subfields, e.g. the maximal tamely ramified subextension of $\mathbb{Q}[p]$. What if one asks about ramification only over a single prime $\ell$ with $\ell \neq p$?]

[Note that, as $p$ varies, every Galois number field appears in infinitely many $\mathbb{Q}[p]$, by the Chebotarev density theorem, so each $\mathbb{Q}[p]$ must be quite large in some (unspecified) sense.]

5. (Abelian extensions having no splitting into unramified and totally ramified parts)

This problem is to show that there exists a subfield $L$ of $E = \mathbb{Q}_5(\zeta_5, \zeta_{5^4-1})$ that cannot be written as a compositum of an unramified extension and a totally ramified extension of the $5$-adic field $\mathbb{Q}_5$.

(a) Show that $E$ is the compositum of $\mathbb{Q}_5(\zeta_5)$, which is cyclic totally ramified of degree 4, and $\mathbb{Q}_5(\zeta_{624})$, which is cyclic unramified of degree 4, since $624 = 5^4 - 1$. Conclude that $Gal(E/\mathbb{Q}_5) = \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$ is abelian. [Query: Are the two fields in the compositum linearly disjoint?]

(b) Let $Gal(E/\mathbb{Q}_5) = \langle \sigma \rangle \times \langle \tau \rangle$ where $\mathbb{Q}_5(\zeta_5)$ is fixed field of $\langle \sigma \rangle: \zeta_5 \mapsto (\zeta_5), \zeta_{624} \mapsto (\zeta_{624})^5$ and $\mathbb{Q}(\zeta_{624})$ is the fixed field of $\langle \tau \rangle: \zeta_5 \mapsto (\zeta_5)^2, \zeta_{624} \mapsto \zeta_{624}$. Now let $L$ be the fixed field of $\langle \sigma^2 \tau \rangle$. Since this element has order 4 in $G$, conclude $L/\mathbb{Q}_5$ must be a cyclic extension of degree 4, and $Gal(L/\mathbb{Q}_5) = \mathbb{Z}/4\mathbb{Z}$.

(c) Show that maximal unramified extension of $L$ is $L_u := L \cap \mathbb{Q}(\zeta_{624})$, and that $L_u$ is of degree 2.

(d) Conclude that there is no totally ramified $L_r \subset L$ of degree 2, with $L = L_rL_u$. If there were, then $L$ would be the compositum of two quadratic extensions of $\mathbb{Q}_5$, so have $Gal(L/\mathbb{Q}_5) = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, which is a contradiction.